# *Introduction to Grassmann Manifolds and Quantum Computation*

Kazuyuki FUJII [*]
Department of Mathematical Sciences
Yokohama City University
Yokohama 236-0027
JAPAN

**Abstract**

Geometrical aspects of quantum computing are reviewed elementarily for non-experts and/or graduate students who are interested in both Geometry and Quantum Computation.

In the first half we show how to treat Grassmann manifolds which are very important examples of manifolds in Mathematics and Physics. Some of their applications to Quantum Computation and its efficiency problems are shown in the second half. An interesting current topic of Holonomic Quantum Computation is also covered.

In the Appendix some related advanced topics are discussed.

## 1 Introduction

This is a review article based on lectures given at several universities in Japan and a talk at Numazu-meeting[1]. The aim is to show a somewhat unconventional but fruitful path connecting Geometry and Quantum Computation, and the audience is graduate students and/or non-experts who are interested in both of the disciplines.

The progress of Quantum Computation after the excellent work of P. Shor [28] on prime factorization of integers and the work of L. Grover [12] on quantum data-base searching is very remarkable. These discoveries have given great impacts on scientists. They drove not only theoreticians to finding other quantum algorithms, but also experimentalists to building practical quantum computers. For standard introduction see for example [29], [26], [17] or [13].

The conventional methods of Quantum Computation are more or less algebraic. On the other hand we are interested in geometrical or topological methods. Geometry or

[*] E-mail address: fujii@yokohama-cu.ac.jp

[1] A meeting held by Yoshinori Machida at Numazu College of Technology to discuss recent results on Geometry, Mathematical Physics, String Theory, Quantum Computation, etc.

Topology are crucial to understand mathematical or physical objects from the global point of view.

For general introduction of Geometry and Topology the book [18] is strongly recommended. But in this book the volume calculations of some important manifolds like Grassmann ones or more generally symmetric spaces are missing. They are important in understanding of entanglements or entangled measures. In the first half we show in some detail the volume calculations of Grassmann manifolds. Here let us recall some basic concepts.

A homogeneous space is defined by

$$M \cong G/H,$$

where $G$ is a Lie group and $H$ its subgroup. We are particularly interested in the case where $G$ is a classical group (for example, a unitary group $U(n)$ or an orthogonal group $O(n)$). The complex Grassmann manifold $G_{k,n}(\mathbf{C})$, which is our main concern in this paper, is written as

$$G_{k,n}(\mathbf{C}) \cong \frac{U(n)}{U(k)\times U(n-k)}.$$

The volume of $G_{k,n}$ is expressed in terms of the well-known volume of $U(n)$ (see the following sections),

$$\mathrm{Vol}\,(G_{k,n}(\mathbf{C})) = \frac{\mathrm{Vol}\,(U(n))}{\mathrm{Vol}\,(U(k))\times \mathrm{Vol}\,(U(n-k))}.$$

This is the usual method to obtain the volume of homogeneous spaces.

On the other hand, the volume is obtained by integrating the volume form of Grassmann manifolds (: $dv(Z,Z^\dagger)$) which is expressed in terms of local coordinates (: $Z$) (see the following sections):

$$\mathrm{Vol}(G_{k,n}(\mathbf{C})) = \int_{G_{k,n}(\mathbf{C})} dv(Z,Z^\dagger).$$

Is it really possible (practical) to carry out the integral on the right hand side? As far as we know such a calculation has not been performed except for $k=1$ (case of complex projective spaces). For $k\geq 2$ direct calculation seems to be very complicated. We would like to present this calculation as a challenging problem to the readers.

Let us come back to Quantum Computation (QC briefly).
Gauge theories are widely recognized as the basic ingredients of quantum field theories which enjoy remarkable progress recently, String Theory, M-Theory, F-Theory, etc. Therefore it is very natural to incorporate gauge theoretical ideas to QC; that is construction of "**gauge theoretical**" quantum computation and/or of "**geometric**" quantum computation in our terminology. The merit of geometric (or topological) method of QC may be the stability with respect to the influence from the environment.

In [31] and [22] Zanardi and Rasetti proposed an attractive idea $\cdots$ **Holonomic Quantum Computation** $\cdots$ using the non-abelian Berry phase (quantum holonomy in the mathematical terminology). We introduce this concept in the final section. See also [16] and [24] for another interesting geometric model.

Quantum Computation comprises of many subjects. To give a comprehensive overview is beyond the scope of this article, so we focus our attention on the construction and the efficiency of unitary operations, and give geometric interpretation to them. Here let us make a brief review.

For $n = 2^t$ ($t \in \mathbf{N}$) we set a unitary operation

$$U_f : (\mathbf{C}^2)^{\otimes t} \longrightarrow (\mathbf{C}^2)^{\otimes t} \ ; \ U_f(|a)) = (-1)^{f(a)}|a)$$

where $f$ is a signature function defined by

$$f : \{0, 1, \cdots, n-1\} \longrightarrow \mathbf{Z}_2 = \{0, 1\}, \quad a \mapsto f(a)$$

and

$$\begin{array}{l} |a) \equiv |a_1\rangle \otimes |a_2\rangle \otimes \cdots |a_{t-1}\rangle \otimes |a_t\rangle, \quad a_k \in \mathbf{Z}_2 \\ a = a_1 2^{t-1} + a_2 2^{t-2} + \cdots + a_{t-1} 2 + a_t, \quad 0 \le a \le n-1. \end{array}$$

This operation plays a crucial role in the quantum data-base searching algorithm of Grover, [12] and an important role in quantum computing, in general. Our concern is as follows. Is it possible to construct this operator in an efficient manner (steps polynomial in $t$)? Has such an algorithm been already given in Quantum Computation?

As far as we know this point is rather unclear, [11]. See [1] and [9]. We will discuss this point in some detail .

We would like to construct a road connecting Geometry and Quantum Computation, which is not an easy task. We will show one of such attempts as explicitly as possible. Though results given in this paper are not new, we do hope our presentation offers new perspectives to not only students and/or non-experts but also to experts.

**The contents of this paper are as follows**:

## 2 Grassmann Manifolds

Let $V$ be a $k$-dimensional subspace in $\mathbf{C}^n$ $(0 \le k \le n)$. Then it is well-known in Linear Algebra that there is only one projection $P : \mathbf{C}^n \longrightarrow \mathbf{C}^n$ with $V = P(\mathbf{C}^n)$. Here the projection means $P^2 = P$ and $P^\dagger = P$ in $M(n;\mathbf{C})$.
The Grassmann manifold is in this case defined by all the $k$-dimensional subspaces in $\mathbf{C}^n$, and it is identified with all the projections in $M(n;\mathbf{C})$ with the trace $k$ or the rank $k$ (corresponding to $V = P(\mathbf{C}^n)$). We note that the eigenvalues of a projection are either 0 or 1 (by $P^2 = P$), so the rank of $P$ = trace of $P$. Therefore we arrive at

$$G_{k,n}(\mathbf{C}) = \{P \in M(n;\mathbf{C}) |\ P^2 = P,\ P^\dagger = P \text{ and } \mathrm{tr}P = k\}. \tag{2.1}$$

A comment is in order. In general it is not easy to visualize all the $k$-dimensional subspaces in $\mathbf{C}^n$ except for experts in Geometry. But it is easy even for us to deal with (2.1) as will be shown in the following.
We note that $G_{0,n}(\mathbf{C}) = \{\mathbf{0}_n\}$ and $G_{n,n}(\mathbf{C}) = \{\mathbf{1}_n\}$. In particular $G_{1,n}(\mathbf{C})$ is called a complex projective space and is written as $\mathbf{C}P^{n-1}$. In (2.1) we know a natural symmetry (isomorphism)

$$\kappa : G_{k,n}(\mathbf{C}) \longrightarrow G_{n-k,n}(\mathbf{C}), \quad \kappa(P) = \mathbf{1}_n - P, \tag{2.2}$$

so that we have $G_{k,n}(\mathbf{C}) \cong G_{n-k,n}(\mathbf{C})$.

Now it is easy to see that $P$ can be written as

$$P = AE_kA^{-1} \quad \text{for some } A \in U(n), \tag{2.3}$$

where $E_k$ is a special projection

$$E_k = \begin{pmatrix} \mathbf{1}_k & O \\ O & \mathbf{0}_{n-k} \end{pmatrix}. \tag{2.4}$$

Therefore we have

$$G_{k,n}(\mathbf{C}) = \{AE_kA^{-1} |\ A \in U(n)\}, \tag{2.5}$$

which directly leads to

$$G_{k,n}(\mathbf{C}) \cong \frac{U(n)}{U(k) \times U(n-k)}\ . \tag{2.6}$$

In particular

$$G_{1,n}(\mathbf{C}) = \mathbf{C}P^{n-1} \cong \frac{U(n)}{U(1) \times U(n-1)} \cong \frac{U(n)/U(n-1)}{U(1)} \cong \frac{\mathrm{S}^{2n-1}}{\mathrm{S}^1}\ , \tag{2.7}$$

see (3.2). Here $\mathrm{S}^k$ is the unit sphere in $\mathbf{R}^{k+1}$ and $U(1) = \mathrm{S}^1$. We note that $G_{k,n}(\mathbf{C})$ is a complex manifold (moreover, a Kähler manifold) and its complex dimension is $k(n-k)$.

Next let us introduce local coordinates around $P$ in (2.3). We denote by $M(n-k, k;\mathbf{C})$ the set of all $(n-k) \times k$ - matrices over $\mathbf{C}$ and define a map

$$\mathcal{P} : M(n-k, k;\mathbf{C}) \longrightarrow G_{k,n}(\mathbf{C})$$

as follows :

$$\mathcal{P}(Z)=A\left(\begin{array}{cc}\mathbf{1}_k & -Z^\dagger \\ Z & \mathbf{1}_{n-k}\end{array}\right)\left(\begin{array}{cc}\mathbf{1}_k & O \\ O & \mathbf{0}_{n-k}\end{array}\right)\left(\begin{array}{cc}\mathbf{1}_k & -Z^\dagger \\ Z & \mathbf{1}_{n-k}\end{array}\right)^{-1}A^{-1}. \tag{2.8}$$

Of course $\mathcal{P}(\mathbf{0})=P$ in (2.3).
Here a natural question arises. How many local coordinates do we have on $G_{k,n}(\mathbf{C})$ ? The number of them is just ${}_nC_k$.
A comment is in order. We believe that this is the best choice of local coordinates on the Grassmann manifold, and this one is called the Oike coordinates in Japan. As far as the author knows H. Oike is the first to write down (2.8), [19].
From this we can show the curvature form $\mathcal{P}(Z)d\mathcal{P}(Z)\wedge d\mathcal{P}(Z)$:

$$d\mathcal{P}(Z)=A\left(\begin{array}{cc}\mathbf{1}_k & -Z^\dagger \\ Z & \mathbf{1}_{n-k}\end{array}\right)\left(\begin{array}{cc}\mathbf{0}_k & {\Lambda_k}^{-1}dZ^\dagger \\ {M_{n-k}}^{-1}dZ & \mathbf{0}_{n-k}\end{array}\right)\left(\begin{array}{cc}\mathbf{1}_k & -Z^\dagger \\ Z & \mathbf{1}_{n-k}\end{array}\right)^{-1}A^{-1}, \tag{2.9}$$

$$\begin{aligned}&\mathcal{P}(Z)d\mathcal{P}(Z)\wedge d\mathcal{P}(Z)\\ &=A\left(\begin{array}{cc}\mathbf{1}_k & -Z^\dagger \\ Z & \mathbf{1}_{n-k}\end{array}\right)\left(\begin{array}{cc}{\Lambda_k}^{-1}dZ^\dagger\wedge{M_{n-k}}^{-1}dZ & O \\ O & \mathbf{0}_{n-k}\end{array}\right)\left(\begin{array}{cc}\mathbf{1}_k & -Z^\dagger \\ Z & \mathbf{1}_{n-k}\end{array}\right)^{-1}A^{-1},\end{aligned} \tag{2.10}$$

where

$$\Lambda_k=\mathbf{1}_k+Z^\dagger Z\in M(k;\mathbf{C}),\quad M_{n-k}=\mathbf{1}_{n-k}+ZZ^\dagger\in M(n-k;\mathbf{C}). \tag{2.11}$$

In the following we omit the $\wedge$ symbol and write, for example, $\mathcal{P}d\mathcal{P}d\mathcal{P}$ instead of $\mathcal{P}(Z)d\mathcal{P}(Z)\wedge d\mathcal{P}(Z)$ for simplicity. A (global) symplectic 2-form on $G_{k,n}(\mathbf{C})$ is given by

$$\omega=\mathrm{tr}\mathcal{P}d\mathcal{P}d\mathcal{P}$$

and its local form

$$\omega=\mathrm{tr}\left(\Lambda_k^{-1}dZ^\dagger M_{n-k}^{-1}dZ\right)=\mathrm{tr}\left((\mathbf{1}_k+Z^\dagger Z)^{-1}dZ^\dagger(\mathbf{1}_{n-k}+ZZ^\dagger)^{-1}dZ\right). \tag{2.12}$$

We want to rewrite (2.12). Before doing this let us make some mathematical preliminaries. For $A\in M(m,\mathbf{C})$ and $B\in M(n,\mathbf{C})$ a tensor product $A\otimes B$ of $A$ and $B$ is defined as

$$A\otimes B=(a_{ij}B)\quad\text{for } A=(a_{ij})\text{ and } B=(b_{pq}).$$

For example, for

$$A=\left(\begin{array}{cc}a_{11} & a_{12}\\ a_{21} & a_{22}\end{array}\right)\quad\text{and}\quad B=\left(\begin{array}{cc}b_{11} & b_{12}\\ b_{21} & b_{22}\end{array}\right)$$

we have

$$A\otimes B=\left(\begin{array}{cc}a_{11}B & a_{12}B\\ a_{21}B & a_{22}B\end{array}\right)=\left(\begin{array}{cccc}a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12}\\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22}\\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12}\\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22}\end{array}\right). \tag{2.13}$$

Therefore componentwise we have $(A \otimes B)_{ip,jq} = A_{ij}B_{pq}$. Then it is not difficult to see

$$\mathrm{tr}(A \otimes B) = \mathrm{tr}(A)\mathrm{tr}(B), \quad \det(A \otimes B) = \{\det(A)\}^n \{\det(B)\}^m. \tag{2.14}$$

Let us construct a column vector $\widehat{Z}$ in $\mathbf{C}^{k(n-k)}$ from $Z$ in $M(n-k,k;\mathbf{C})$ in a usual manner:

$$\widehat{Z} = (z_{11}, \cdots, z_{1k}, \cdots\cdots, z_{n-k,1}, \cdots, z_{n-k,k})^T \ ,$$

where $T$ means a transpose. Now we rewrite (2.12) as follows:

$$\begin{aligned}\omega &= \mathrm{tr}\left(\Lambda_k^{-1} dZ^\dagger M_{n-k}^{-1} dZ\right) = \mathrm{tr}\left(dZ^\dagger M_{n-k}^{-1} dZ \Lambda_k^{-1}\right) \\ &= \sum (dZ^\dagger)_{ij}(M_{n-k}^{-1})_{jp}(dZ)_{pq}(\Lambda_k^{-1})_{qi} = \sum d\bar{z}_{ji}(M_{n-k}^{-1})_{jp} dz_{pq}(\Lambda_k^{-1})_{qi} \\ &= \sum d\bar{z}_{ji}(M_{n-k}^{-1})_{jp}(\Lambda_k^{-1})_{qi} dz_{pq} = \sum d\bar{z}_{ji}(M_{n-k}^{-1})_{jp}(\Lambda_k^{-1})^T{}_{iq} dz_{pq} \\ &= \sum (d\widehat{Z}^\dagger)_{ji} \left\{M_{n-k}^{-1} \otimes (\Lambda_k^{-1})^T\right\}_{ji,pq} d\widehat{Z}_{pq} = (d\widehat{Z})^\dagger \left\{M_{n-k}^{-1} \otimes (\Lambda_k^{-1})^T\right\} d\widehat{Z}. \end{aligned} \tag{2.15}$$

The symplectic volume on $G_{k,n}(\mathbf{C})$ which coincides with the usual volume is given by

$$dv = \frac{1}{\{k(n-k)\}!}\left(\frac{\omega}{2\sqrt{-1}}\right)^{k(n-k)}. \tag{2.16}$$

Here $\frac{1}{2\sqrt{-1}}$ is a normalization factor. From (2.15) it is easy to see

$$\omega^{k(n-k)} = \{k(n-k)\}! \det\left\{M_{n-k}^{-1} \otimes (\Lambda_k^{-1})^T\right\} \prod_{i,j} d\bar{z}_{ij} dz_{ij}. \tag{2.17}$$

Therefore (2.16) becomes

$$dv = \det\left\{M_{n-k}^{-1} \otimes (\Lambda_k^{-1})^T\right\} \prod_{i,j} \frac{d\bar{z}_{ij} dz_{ij}}{2\sqrt{-1}}. \tag{2.18}$$

On the other hand by (2.14) we have

$$\det\left\{M_{n-k}^{-1} \otimes (\Lambda_k^{-1})^T\right\} = \left(\det M_{n-k}^{-1}\right)^k \left(\det(\Lambda_k^{-1})\right)^{n-k} = (\det M_{n-k})^{-k} (\det \Lambda_k)^{-(n-k)}. \tag{2.19}$$

Here we note $\det\Lambda_k = \det M_{n-k}$. For

$$X = \begin{pmatrix} \mathbf{1}_k & -Z^\dagger \\ Z & \mathbf{1}_{n-k} \end{pmatrix},$$

we have

$$\det X = \det \begin{pmatrix} \mathbf{1}_k & -Z^\dagger \\ Z & \mathbf{1}_{n-k} \end{pmatrix} = \det \begin{pmatrix} \mathbf{1}_k + Z^\dagger Z & -Z^\dagger \\ O & \mathbf{1}_{n-k} \end{pmatrix} = \det\left(\mathbf{1}_k + Z^\dagger Z\right) = \det\Lambda_k.$$

On the other hand

$$\det X = \det \begin{pmatrix} \mathbf{1}_k & -Z^\dagger \\ Z & \mathbf{1}_{n-k} \end{pmatrix} = \det \begin{pmatrix} \mathbf{1}_k & -Z^\dagger \\ O & \mathbf{1}_{n-k} + ZZ^\dagger \end{pmatrix} = \det\left(\mathbf{1}_{n-k} + ZZ^\dagger\right) = \det M_{n-k},$$

so that

$$\det\Lambda_k = \det M_{n-k} \quad \blacksquare$$

From (2.19) $\det\left\{M_{n-k}^{-1}\otimes(\Lambda_k^{-1})^T\right\} = (\det\Lambda_k)^{-n}$, so we arrive at

$$dv(Z,Z^\dagger) = (\det\Lambda_k)^{-n}\prod_{i,j}\frac{d\bar{z}_{ij}dz_{ij}}{2\sqrt{-1}} = \left\{\det(\mathbf{1}_k + Z^\dagger Z)\right\}^{-n}\prod_{i,j}\frac{d\bar{z}_{ij}dz_{ij}}{2\sqrt{-1}}. \tag{2.20}$$

From the above-mentioned facts the volume of Grassmann manifold $G_{k,n}(\mathbf{C})$ is given as

$$\mathrm{Vol}(G_{k,n}(\mathbf{C})) = \int_{M(n-k,k;\mathbf{C})}\frac{\prod_{i,j}\frac{d\bar{z}_{ij}dz_{ij}}{2\sqrt{-1}}}{\{\det(\mathbf{1}_k + Z^\dagger Z)\}^n}\ . \tag{2.21}$$

**Problem** How can we calculate this integral ?

# 3 Volume of Unitary Groups

Here we will show a heuristic method of evaluation of the volume of unitary group $U(n)$. Let $S^{2k-1}$ be the $2k-1$ - dimensional unit sphere ($k \geq 1$) over $\mathbf{R}$ and the volume be $\mathrm{Vol}(S^{2k-1})$. For example $\mathrm{Vol}(S^1) = 2\pi$ and $\mathrm{Vol}(S^3) = 2\pi^2$. In general we have

$$\mathrm{Vol}(S^{2k-1}) = \frac{2\pi^k}{(k-1)!}. \tag{3.1}$$

Since we know the fact

$$\frac{U(k)}{U(k-1)} \cong S^{2k-1}, \tag{3.2}$$

we have

$$\begin{aligned} U(n) &\doteq \frac{U(n)}{U(n-1)}\times\frac{U(n-1)}{U(n-2)}\times\cdots\times\frac{U(2)}{U(1)}\times U(1) \\ &\doteq S^{2n-1}\times S^{2n-3}\times\cdots\times S^3\times S^1, \end{aligned} \tag{3.3}$$

where $\doteq$ means **almost equal**!

A comment is in order. Of course the equality does not hold in (3.3) except for the cases of $n = 1,\ 2$. But for the purpose of volume-counting or cohomology-counting there is no problem to use (3.3)[2].

By combining (3.3) and (3.1) we obtain

$$\mathrm{Vol}(U(n)) = \prod_{j=1}^{n}\mathrm{Vol}(S^{2j-1}) = \prod_{j=1}^{n}\frac{2\pi^j}{(j-1)!} = \frac{2^n\pi^{\frac{n(n+1)}{2}}}{0!1!\cdots(n-1)!}. \tag{3.4}$$

Let us evaluate the volume of Grassmann manifold $G_{k,n}(\mathbf{C})$:

$$G_{k,n}(\mathbf{C}) \cong \frac{U(n)}{U(k)\times U(n-k)} \Longrightarrow \mathrm{Vol}(G_{k,n}(\mathbf{C})) = \frac{\mathrm{Vol}(U(n))}{\mathrm{Vol}(U(k))\times\mathrm{Vol}(U(n-k))}.$$

[2] You will know this "questionable equation" may be rather useful, see for example [25].

From (3.4) we obtain

$$
\begin{aligned}
\mathrm{Vol}(G_{k,n}(\mathbf{C})) &= \frac{0!1!\cdots(k-1)!\ 0!1!\cdots(n-k-1)!}{0!1!\cdots\cdots(n-1)!}\pi^{k(n-k)} \\
&= \frac{0!1!\cdots(k-1)!}{(n-k)!\cdots(n-2)!(n-1)!}\pi^{k(n-k)}.
\end{aligned} \tag{3.5}
$$

# 4 A Question

Combining (2.21) with (3.5) we have the main result

$$
\int_{M(n-k,k;\mathbf{C})} \frac{\prod_{i,j}\frac{d\bar{z}_{ij}dz_{ij}}{2\sqrt{-1}}}{\{\det(\mathbf{1}_k + Z^{\dagger}Z)\}^n} \;=\; \frac{0!1!\cdots(k-1)!}{(n-k)!\cdots(n-2)!(n-1)!}\pi^{k(n-k)}. \tag{4.1}
$$

It has to be emphasized that the right hand side has been obtained by an indirect path. Is it really easy (or practical) to carry out the integration to obtain the right hand side? As far as we know, the integral has not been calculated except for the case $k = 1$.

Let us review the case $k = 1$:

$$
\int_{\mathbf{C}^{n-1}} \frac{1}{(1+\sum_{j=1}^{n-1}|z_j|^2)^n}\prod_{j=1}^{n-1}\frac{d\bar{z}_j dz_j}{2\sqrt{-1}} \;=\; \frac{\pi^{n-1}}{(n-1)!}\ . \tag{4.2}
$$

The proof is as follows. First let us make a change of variables:

$$
z_j = \sqrt{r_j}\mathrm{e}^{\sqrt{-1}\theta_j} \quad \text{for } 1 \le j \le n-1. \tag{4.3}
$$

Then we have easily

$$
\frac{d\bar{z}_j dz_j}{2\sqrt{-1}} = \frac{1}{2}dr_j d\theta_j.
$$

Under this change of variables (4.2) becomes

$$
(4.2) = \int_0^{2\pi}\int_0^{\infty}\frac{1}{(1+\sum_{j=1}^{n-1}r_j)^n}\prod_{j=1}^{n-1}\frac{d\theta_j}{2}\prod_{j=1}^{n-1}dr_j = \pi^{n-1}\int_0^{\infty}\frac{1}{(1+\sum_{j=1}^{n-1}r_j)^n}\prod_{j=1}^{n-1}dr_j.
$$

Here let us once more make a change of variables from $(r_1,\cdots,r_{n-1})$ to $(\xi_1,\cdots,\xi_{n-1})$:

$$
\begin{aligned}
r_1 &= \xi_1(1-\xi_2), \\
r_2 &= \xi_1\xi_2(1-\xi_3), \\
&\ \vdots \qquad\qquad \vdots \\
r_{n-2} &= \xi_1\xi_2\cdots\xi_{n-2}(1-\xi_{n-1}), \\
r_{n-1} &= \xi_1\xi_2\cdots\xi_{n-2}\xi_{n-1}.
\end{aligned}
$$

Conversely we have

$$\begin{aligned}
\xi_1 &= r_1 + r_2 + \cdots + r_{n-2} + r_{n-1}, \\
\xi_2 &= \frac{r_2 + \cdots + r_{n-2} + r_{n-1}}{r_1 + r_2 + \cdots + r_{n-2} + r_{n-1}}, \\
\vdots & \qquad \vdots \\
\xi_{n-2} &= \frac{r_{n-2} + r_{n-1}}{r_{n-3} + r_{n-2} + r_{n-1}}, \\
\xi_{n-1} &= \frac{r_{n-1}}{r_{n-2} + r_{n-1}}, \\
& 0 \le \xi_1 < \infty, \quad 0 \le \xi_2, \cdots, \xi_{n-1} \le 1, \\
& \prod_{j=1}^{n-1} dr_j = {\xi_1}^{n-2} {\xi_2}^{n-3} \cdots \xi_{n-2} \prod_{j=1}^{n-1} d\xi_j .
\end{aligned}$$

Under this change of variables (4.2) becomes

$$\begin{aligned}
(4.2) &= \pi^{n-1} \int_0^\infty \frac{{\xi_1}^{n-2}}{(1+\xi_1)^n} d\xi_1 \int_0^1 {\xi_2}^{n-3} d\xi_2 \cdots \int_0^1 \xi_{n-2} d\xi_{n-2} \\
&= \pi^{n-1} \int_0^1 {\xi_1}^{n-2} d\xi_1 \int_0^1 {\xi_2}^{n-3} d\xi_2 \cdots \int_0^1 \xi_{n-2} d\xi_{n-2} \\
&= \pi^{n-1} \frac{1}{n-1} \frac{1}{n-2} \cdots \frac{1}{2} = \frac{\pi^{n-1}}{(n-1)!} \quad \blacksquare \qquad (4.4)
\end{aligned}$$

The direct proof of (4.1) for $k = 1$ is relatively easy as shown above. But for $k \ge 2$ we do not know such a proof (a direct proof may be very complicated). Therefore let us present

**Problem** Give a direct proof to

$$\int_{M(n-k,k;\mathbf{C})} \frac{\prod_{i,j} \frac{d\bar{z}_{ij} dz_{ij}}{2\sqrt{-1}}}{\{\det(\mathbf{1}_k + Z^\dagger Z)\}^n} = \frac{0!1! \cdots (k-1)!}{(n-k)! \cdots (n-2)!(n-1)!} \pi^{k(n-k)}.$$

As for another approach to the above problem we refer to [10]. In this paper coherent states based on Grassmann manifolds have been constructed.

# 5 Quantum Computing

Let us move to the main subject of Quantum Computing. The typical examples of quantum algorithms up to now are

- Factoring algorithm of integers by P. Shor [28],
- Quantum data-base searching algorithm by L. Grover [12].

See [29] and [26], or [17] for general introduction. [14] and [15] are also recommended.

In Quantum Computing we in general expect an exponential speedup compared to classical ones, so we must construct necessarily unitary matrices in $U(n)$ in an efficient manner when $n$ is a huge number like $2^{100}$.

**Problem** How can we construct unitary matrices in an efficient manner?

Let us come back to (2.1). We denote the set of $n \times n$ projection operators by

$$G_n(\mathbf{C}) = \{P \in M(n;\mathbf{C}) |\ P^2 = P,\ P^\dagger = P\}. \tag{5.1}$$

The elements of $G_n(\mathbf{C})$ are classified by the trace, so $G_n(\mathbf{C})$ can be decomposed into a disjoint union

$$G_n(\mathbf{C}) = \bigcup_{k=0}^{n} G_{k,n}(\mathbf{C}). \tag{5.2}$$

For a $k$-dimensional subspace $V$ in $\mathbf{C}^n$ $(0 \le k \le n)$ let $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k\}$ be an orthonormal basis (namely, $< \mathbf{v}_i, \mathbf{v}_j >= \delta_{ij}$) and set

$$V = (\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k) \in M(n,k;\mathbf{C}). \tag{5.3}$$

We have identified a $k$-dimensional subspace $V$ with a matrix $V$ in (5.3) for simplicity (maybe there is no confusion). Then we have an equivalence

$$\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k\} : \text{orthonormal} \ \Leftrightarrow\ V^\dagger V = \mathbf{1}_k.$$

Then it is easy to see that all orthonormal basis in $V$ are given by

$$\{Va |\ a \in U(k)\}. \tag{5.4}$$

The projection corresponding to $V$ is written by

$$P = VV^\dagger \in G_{k,n}(\mathbf{C}). \tag{5.5}$$

We remark that $(Va)(Va)^\dagger = Vaa^\dagger V^\dagger = VV^\dagger = P$, namely $P$ is of course independent of $a \in U(k)$. This $P$ is also expressed as

$$P = \sum_{j=1}^{k} \mathbf{v}_j {\mathbf{v}_j}^\dagger. \tag{5.6}$$

If we use Dirac's bra-ket notation $\mathbf{v}_j = |j\rangle$, then $P = \sum_{j=1}^{k} |j\rangle\langle j|$. This notation may be popular in Physics rather than (5.6).

How can we construct an element of unitary group from an element of Grassmann manifolds? We have a canonical method, namely

$$G_n(\mathbf{C}) \longrightarrow U(n) : P \longmapsto U = 1_n - 2P. \tag{5.7}$$

This $U$ is called a uniton in the field of harmonic maps. Moreover we can consider a product of some unitons, namely, for any $S \subset \{0, 1, \cdots, n-1, n\}$

$$U = \prod_{j \in S} (1_n - 2P_j) \quad \text{for } P_j \in G_{j,n}(\mathbf{C}). \tag{5.8}$$

In particular

$$U = \prod_{j=1}^{n-1} (1_n - 2P_j) \quad \text{for } P_j \in G_{j,n}(\mathbf{C}) \tag{5.9}$$

is very important in the field of harmonic maps, see for example [4] and [30].
Many important unitary matrices are made by this way[3].

These unitary matrices also play an important role in Quantum Computing as shown in the following.

We consider a qubit (**qu**antum **bit**) space of quantum particles. The 1-qubit space is identified with $\mathbf{C}^2$ with basis $\{|0\rangle, |1\rangle\}$ ;

$$\mathbf{C}^2 = \mathrm{Vect}_{\mathbf{C}}\{|0\rangle, |1\rangle\}, \quad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} .$$

The qubit space of $t$-particles is the **tensor product** (not direct sum!) of $\mathbf{C}^2$

$$\mathbf{C}^2 \otimes \mathbf{C}^2 \otimes \cdots \otimes \mathbf{C}^2 \equiv (\mathbf{C}^2)^{\otimes t} \tag{5.10}$$

with basis

$$\{|n_1, n_2, \ldots, n_t\rangle = |n_1\rangle \otimes |n_2\rangle \otimes \cdots \otimes |n_t\rangle \mid n_j \in \mathbf{Z}_2 = \{0, 1\} \} .$$

For example,

$$|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \ |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \ |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \ |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Now we take the Walsh-Hadamard transformation $W$ defined by

$$W : |0\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad W : |1\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{5.11}$$

in matrix notation,

$$W = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in O(2) \subset U(2). \tag{5.12}$$

[3] Those used in [2] for data-base searching algorithms are of this form with appropriate $P_j$.

This transformation (or matrix) is unitary and it plays a very important role in Quantum Computing. Moreover is easy to realize it in Quantum Optics. Let us list some important properties of $W$:

$$W^2 = \mathbf{1}_2, \quad W^\dagger = W = W^{-1}, \tag{5.13}$$

$$\sigma_1 = W\sigma_3 W^{-1}, \tag{5.14}$$

where $\{\sigma_1, \sigma_2, \sigma_3\}$ are the Pauli matrices:

$$\sigma_1 = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, \ \sigma_2 = \begin{pmatrix} & -\sqrt{-1} \\ \sqrt{-1} & \end{pmatrix}, \ \sigma_3 = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}. \tag{5.15}$$

See Appendix **B** for a generalization of Pauli matrices. Next we consider $t$-tensor product of $W$ $(t \in \mathbf{N})$ :

$$W^{\otimes t} = W \otimes W \otimes \cdots \otimes W \ (t\text{-times}). \tag{5.16}$$

This matrix of course operates on the space (5.10). For example

$$W \otimes W = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \tag{5.17}$$

and

$$W \otimes W \otimes W = \frac{1}{\sqrt{8}}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}. \tag{5.18}$$

Hereafter we set $n = 2^t$. Then (5.16) means $W^{\otimes t} \in U(n)$. The very important fact is that (5.16) can be constructed by only $t(= \log_2(n))$-steps in Quantum Computing. Let us show the matrix-component of (5.16) is given by

$$\langle i_1, i_2, \ldots, i_t | W^{\otimes t} | j_1, j_2, \ldots, j_t \rangle = \frac{1}{\sqrt{n}}(-1)^{\sum_{k=1}^{t} i_k j_k} \tag{5.19}$$

or if we set

$$|i) = |i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_t\rangle, \quad i = i_1 2^{t-1} + i_2 2^{t-2} + \cdots + i_t, \quad 0 \le i \le n-1$$

we have

$$(i|W^{\otimes t}|j) = \frac{1}{\sqrt{n}}(-1)^{i \cdot j} \tag{5.20}$$

where $i \cdot j$ means the sum of bit-wise products $\sum_{k=1}^{t} i_k j_k$.

The proof goes as follows. From (5.12) we know

$$W|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^i|1\rangle) = \frac{1}{\sqrt{2}}\sum_{k=0}^{1}(-1)^{ik}|k\rangle,$$

which implies

$$\begin{aligned} W^{\otimes t}|j) &= W|j_1\rangle \otimes W|j_2\rangle \otimes \cdots \otimes W|j_t\rangle \\ &= \frac{1}{\sqrt{2^t}}\sum_{k_1=0}^{1}\sum_{k_2=0}^{1}\cdots\sum_{k_t=0}^{1}(-1)^{k_1j_1+k_2j_2+\cdots+k_tj_t}|k_1\rangle \otimes |k_2\rangle \otimes \cdots |k_t\rangle \\ &= \frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}(-1)^{k\cdot j}|k). \end{aligned} \tag{5.21}$$

Therefore we obtain

$$(i|W^{\otimes t}|j) = \frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}(-1)^{k\cdot j}(i|k) = \frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}(-1)^{k\cdot j}\delta_{ik} = \frac{1}{\sqrt{n}}(-1)^{i\cdot j} \quad \blacksquare$$

Moreover (5.16) has an interesting property which we can guess from (5.17) and (5.18):

$$\sum_{j=0}^{n-1}(i|W^{\otimes t}|j) = \begin{cases} \sqrt{n}, & \text{if } \ i=0 \\ 0, & \text{othewise} \end{cases} \tag{5.22}$$

or

$$\sum_{i=0}^{n-1}(i|W^{\otimes t}|j) = \begin{cases} \sqrt{n}, & \text{if } \ j=0 \\ 0, & \text{othewise.} \end{cases} \tag{5.23}$$

Let us clarify the meaning of (5.20) from the point of view of Group Theory.
We note that $\mathbf{Z}_2$ is an abelian group with operation $\oplus$

$$0 \oplus 0 = 0,\ 0 \oplus 1 = 1,\ 1 \oplus 0 = 1,\ 1 \oplus 1 = 0. \tag{5.24}$$

Then ${\mathbf{Z}_2}^t$ is a natural product group of $\mathbf{Z}_2$. We denote its element by

$$\mathbf{i} = (i_1, i_1, \cdots, i_t) \longleftrightarrow i = i_1 2^{t-1} + i_2 2^{t-2} + \cdots + i_t.$$

For $\mathbf{i} \in {\mathbf{Z}_2}^t$ we define

$$\chi_{\mathbf{i}} : {\mathbf{Z}_2}^t \longrightarrow \mathbf{C}^* = \mathbf{C} - \{0\}, \quad \chi_{\mathbf{i}}(\mathbf{j}) = \sqrt{n}(i|W^{\otimes t}|j) = (-1)^{i\cdot j}. \tag{5.25}$$

Then we can show that

$$\chi_{\mathbf{i}}(\mathbf{j} \oplus \mathbf{k}) = \chi_{\mathbf{i}}(\mathbf{j})\chi_{\mathbf{i}}(\mathbf{k}). \tag{5.26}$$

That is, $\chi_{\mathbf{i}}$ is a character of the abelian group ${\mathbf{Z}_2}^t$.
The proof is as follows. From (5.24) we know

$$x \oplus y = x + y - 2xy \quad \text{for } \ x, y \in \mathbf{Z}_2. \tag{5.27}$$

Therefore we obtain

$$\begin{aligned}\chi_{\mathbf{i}}(\mathbf{j}\oplus\mathbf{k}) &= (-1)^{\sum_{l=1}^{t} i_l(j_l\oplus k_l)} = (-1)^{\sum_{l=1}^{t} i_l(j_l+k_l-2j_lk_l)} = (-1)^{\sum_{l=1}^{t} i_l(j_l+k_l)} \\ &= (-1)^{\sum_{l=1}^{t} i_lj_l}(-1)^{\sum_{l=1}^{t} i_lk_l} = (-1)^{i\cdot j}(-1)^{i\cdot k} = \chi_{\mathbf{i}}(\mathbf{j})\chi_{\mathbf{i}}(\mathbf{k}) \quad \blacksquare \qquad (5.28)\end{aligned}$$

These characters play an important role in Discrete Fourier Transform, see [14] or recent preprint [15].

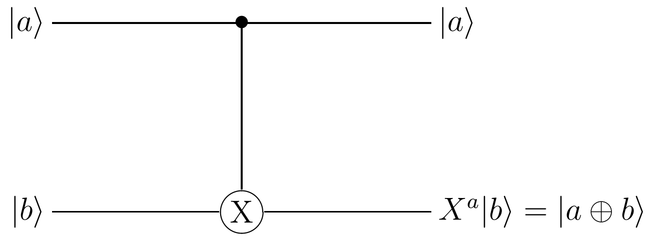
Now we consider a controlled NOT operation (gate) which we will denote by C-NOT in the following. It is defined by

$$\begin{aligned}\text{C-NOT}: \quad &|0,0\rangle \rightarrow |0,0\rangle, \quad |0,1\rangle \rightarrow |0,1\rangle, \\ &|1,0\rangle \rightarrow |1,1\rangle, \quad |1,1\rangle \rightarrow |1,0\rangle \qquad (5.29)\end{aligned}$$

or more compactly

$$\text{C-NOT}: |a,b\rangle \longrightarrow |a, a\oplus b\rangle, \quad a,\ b\in\mathbf{Z}_2. \qquad (5.30)$$

Graphically it is expressed as



and the matrix representation is

$$\text{C-NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \qquad (5.31)$$

Here $a\oplus b = a+b \pmod 2$ and we note the relation

$$X^a|b\rangle \equiv \sigma_1^a|b\rangle = |a\oplus b\rangle \quad \text{for} \quad a,\ b\in\mathbf{Z}_2. \qquad (5.32)$$

In this case the first bit is called a control bit and the second a target bit.
Of course we can consider the reverse case. Namely, the first bit is a target one and the second a control one, which is also called the controlled NOT operation:

$$\text{C-NOT}: |a,b\rangle \longrightarrow |a\oplus b, b\rangle, \quad a,\ b\in\mathbf{Z}_2, \qquad (5.33)$$

and the matrix representation is

$$\text{C-NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \qquad (5.34)$$

A comment is in order. In the 1-qubit case we may assume that we can construct all unitary operations in $U(2)$ (we call the operation universal). In the 2-qubit case how can we construct all unitary operations in $U(4)$? If we can construct the C-NOT (5.31), (5.34) in our system, then we can show the operation is universal, see [3] and [1]. This is a crucial point in quantum computing. We comment here that the C-NOT (5.31) can be written as a uniton (5.7)

$$\text{C-NOT} = \mathbf{1}_4 - 2P \tag{5.35}$$

where

$$P = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix}, \tag{5.36}$$

and this $P$ can be diagonalized by making use of Walsh-Hadamard transformation (5.12) like

$$P = (\mathbf{1}_2 \otimes W)\widetilde{E}_1(\mathbf{1}_2 \otimes W)^{-1} = (\mathbf{1}_2 \otimes W)(\sigma_1 \otimes \sigma_1)E_1(\sigma_1 \otimes \sigma_1)^{-1}(\mathbf{1}_2 \otimes W)^{-1} \tag{5.37}$$

where

$$\widetilde{E}_1 = \begin{pmatrix} 0 & & & \\ & 0 & & \\ & & 0 & \\ & & & 1 \end{pmatrix}, \qquad E_1 = \begin{pmatrix} 1 & & & \\ & 0 & & \\ & & 0 & \\ & & & 0 \end{pmatrix}. \tag{5.38}$$

More generally for the $t$-qubit case we can construct $(t-1)$-repeated controlled-not operator and show it is a uniton.

The $(t-1)$-repeated controlled-not operation is defined by

$$\begin{aligned} \text{C}^{(t-1)}\text{-NOT} : |a_1, a_2, \cdots, a_{t-1}, a_t\rangle \longrightarrow & |a_1, a_2, \cdots, a_{t-1}, a_1 a_2 \cdots a_{t-1} \oplus a_t\rangle, \\ & a_k \in \mathbf{Z}_2 \quad (k = 1, 2, \cdots, t), \end{aligned} \tag{5.39}$$

or in matrix form

$$\text{C}^{(t-1)}\text{-NOT} = \begin{pmatrix} 1 & & & & & \\ & \cdot & & & & \\ & & \cdot & & & \\ & & & 1 & & \\ & & & & 0 & 1 \\ & & & & 1 & 0 \end{pmatrix} : \quad 2^t \times 2^t - \text{matrix}. \tag{5.40}$$

As for the explicit construction of $(t-1)$-repeated controlled-not operator see [1] or [9]. See also Appendix. But unfortunately the construction is not **efficient** !
A comment is in order. In [1] a rough estimation of the number of steps to construct the operator (5.39) is given and it is confirmed that an efficient construction is possible. But no explicit construction is given.

By the way, since

$$\mathbf{1}_2{}^{\otimes(t-1)} \otimes W = \begin{pmatrix} W & & & & \\ & \cdot & & & \\ & & \cdot & & \\ & & & W & \\ & & & & W \end{pmatrix}, \tag{5.41}$$

we have

$$\begin{aligned} \left(\mathbf{1}_2{}^{\otimes(t-1)} \otimes W\right) \mathrm{C}^{(t-1)}\text{-NOT} \left(\mathbf{1}_2{}^{\otimes(t-1)} \otimes W\right) &= \begin{pmatrix} 1 & & & & & \\ & \cdot & & & & \\ & & \cdot & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & -1 \end{pmatrix} \\ &= \mathbf{1}_n - 2|n-1)(n-1|. \end{aligned} \tag{5.42}$$

Therefore the construction of $\mathrm{C}^{(t-1)}$-NOT and $\mathbf{1}_n - 2|n-1)(n-1|$ have almost the same number of steps. Is it possible to construct this operator efficiently ?
As far as we know an explicit and efficient construction of this operation has not yet been given[4].

**Problem** Give an explicit and efficient algorithm to this operation.

Let us consider a set

$$\{F_k \mid 1 \le k \le n\} \tag{5.43}$$

where

$$F_k = \mathbf{1}_n - 2E_k = \begin{pmatrix} -\mathbf{1}_k & \\ & \mathbf{1}_{n-k} \end{pmatrix}.$$

If $F_1$ can be constructed, then the other $F$'s can be easily obtained. First let us show this with a simple example ($t$=2) :

$$F_1 = \begin{pmatrix} -1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} = \mathbf{1}_4 - 2|0)(0|.$$

Now we set

$$U_1 = \mathbf{1}_2 \otimes \sigma_1 = \begin{pmatrix} & 1 & & \\ 1 & & & \\ & & & 1 \\ & & 1 & \end{pmatrix}, \quad U_2 = \sigma_1 \otimes \mathbf{1}_2 = \begin{pmatrix} & & 1 & \\ & & & 1 \\ 1 & & & \\ & 1 & & \end{pmatrix},$$

$$U_3 = \sigma_1 \otimes \sigma_1 = \begin{pmatrix} & & & 1 \\ & & 1 & \\ & 1 & & \\ 1 & & & \end{pmatrix},$$

[4] I have not yet succeeded in such a construction.

then we have

$$U_1F_1U_1 = \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} = \mathbf{1}_4 - 2|1)(1|,$$
$$U_2F_1U_2 = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & 1 \end{pmatrix} = \mathbf{1}_4 - 2|2)(2|,$$
$$U_3F_1U_3 = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix} = \mathbf{1}_4 - 2|3)(3|,$$

so that it is easy to check

$$F_1\,(U_1F_1U_1) = F_2,\ \ F_2\,(U_2F_1U_2) = F_3 \ \text{ and } \ F_3\,(U_3F_1U_3) = -\mathbf{1}_4. \tag{5.44}$$

Let us prove the general case. For $i = i_1 2^{t-1} + i_2 2^{t-2} + \cdots + i_t$ $(0 \le i \le n-1)$ we set

$$U_i = \sigma_1^{i_1} \otimes \sigma_1^{i_2} \otimes \cdots \otimes \sigma_1^{i_t}, \quad (U_i^\dagger = U_i = U_i^{-1}). \tag{5.45}$$

Since

$$\begin{aligned} U_i|0) &= \sigma_1^{i_1} \otimes \sigma_1^{i_2} \otimes \cdots \otimes \sigma_1^{i_t}\ (|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle) \\ &= \sigma_1^{i_1}|0\rangle \otimes \sigma_1^{i_2}|0\rangle \otimes \cdots \otimes \sigma_1^{i_t}|0\rangle \\ &= |i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_t\rangle \equiv |i), \end{aligned} \tag{5.46}$$

we have

$$\mathbf{1}_n - 2|i)(i| = U_i\left(\mathbf{1}_n - 2|0)(0|\right)U_i = U_iF_1U_i. \tag{5.47}$$

Therefore it is easy to see that

$$F_k\,(U_kF_1U_k) = F_{k+1} \quad (1 \le k \le n-1). \quad \blacksquare \tag{5.48}$$

We note that this procedure is not efficient.

Now, let us make a comment on Grover's data-base searching algorithm. In his algorithm the following two unitary operations play an essential role:

$$\mathbf{1}_n - 2|i)(i|, \quad \mathbf{1}_n - 2|s)(s|, \tag{5.49}$$

in which the state $|s)$ ($s$ stands for *sum*) is defined by

$$|s) \equiv \frac{1}{\sqrt{n}}\sum_{i=0}^{n-1}|i) = W^{\otimes t}|0). \tag{5.50}$$

We find via (5.21) that

$$\mathbf{1}_n - 2|s)(s| = W^{\otimes t}\left(\mathbf{1}_n - 2|0)(0|\right)W^{\otimes t} = W^{\otimes t}F_1W^{\otimes t}. \tag{5.51}$$

Namely, the two operations (5.49) are both unitons and can be diagonalized by the efficient unitary operations $U_i$ and $W^{\otimes t}$.

Finally, let us mention about a relation between $(t-1)$-repeated controlled- not operation and $F_1$. Since

$$\left(\mathbf{1}_2{}^{\otimes(t-1)} \otimes W\right) \mathrm{C}^{(t-1)}\text{-NOT}\left(\mathbf{1}_2{}^{\otimes(t-1)} \otimes W\right) = \mathbf{1}_n - 2|n-1)(n-1| = U_{n-1}F_1U_{n-1}$$

by (5.42), we have

$$F_1 = U_{n-1}\left(\mathbf{1}_2{}^{\otimes(t-1)} \otimes W\right) \mathrm{C}^{(t-1)}\text{-NOT}\left(\mathbf{1}_2{}^{\otimes(t-1)} \otimes W\right)U_{n-1}.$$

By substituting $U_{n-1} = \sigma_1 \otimes \sigma_1 \otimes \cdots \otimes \sigma_1 \otimes \sigma_1$ into the equation above we arrive at the desired relation

$$F_1 = \left(\sigma_1{}^{\otimes(t-1)} \otimes \sigma_1 W\right) \mathrm{C}^{(t-1)}\text{-NOT}\left(\sigma_1{}^{\otimes(t-1)} \otimes W\sigma_1\right). \tag{5.52}$$

# 6 Holonomic Quantum Computation

In this section we briefly introduce a simplified version of Holonomic Quantum Computation. The full story would require detailed knowledge of Quantum Mechanics, Quantum Optics and Global Analysis, so it will have to wait for another occasion.

This model was proposed by Zanardi and Rasetti [31] and [22] and it has been developed by Fujii [5], [6], [7], [8] and Pachos [20], [21].

This model uses the non-abelian Berry phase (quantum holonomy in the mathematical terminology [18]) in the process of quantum computing. In this model a Hamiltonian (including some parameters) must have certain degeneracy because an adiabatic connection (the non-abelian Berry connection) is introduced in terms of the degeneracy, see [27]. In other words, a quantum computational bundle is introduced on some parameter space due to this degeneracy and the canonical connection of this bundle is just the one above. On this bundle Holonomic Quantum Computation is performed by making use of the holonomy operations. We note our method is completely geometrical.

Here we introduce **quantum computational bundles**, [5], [6], and [8]. For this purpose we need universal principal and vector bundles over infinite dimensional Grassmann manifolds. We also need an infinite dimensional vector space called a Hilbert (or Fock) space.

Let $\mathcal{H}$ be a separable Hilbert space over $\mathbf{C}$. For $m \in \mathbf{N}$, we set

$$St_m(\mathcal{H}) \equiv \left\{V = (v_1, \cdots, v_m) \in \mathcal{H} \times \cdots \times \mathcal{H} \middle| \, V^\dagger V = 1_m\right\}, \tag{6.1}$$

where $1_m$ is a unit matrix in $M(m, \mathbf{C})$. This is called a (universal) Stiefel manifold. Note that the unitary group $U(m)$ acts on $St_m(\mathcal{H})$ from the right:

$$St_m(\mathcal{H}) \times U(m) \to St_m(\mathcal{H}) : (V, a) \mapsto Va. \tag{6.2}$$

Next we define a (universal) Grassmann manifold

$$Gr_m(\mathcal{H}) \equiv \left\{ X \in M(\mathcal{H}) |\ X^2 = X, X^\dagger = X \text{ and } \mathrm{tr}X = m \right\}, \tag{6.3}$$

where $M(\mathcal{H})$ denotes a space of all bounded linear operators on $\mathcal{H}$. Then we have a projection

$$\pi : St_m(\mathcal{H}) \to Gr_m(\mathcal{H}), \quad \pi(V) \equiv VV^\dagger = \sum_{j=1}^{m} v_j v_j^\dagger, \tag{6.4}$$

compatible with the action (6.2) ($\pi(Va) = Va(Va)^\dagger = Vaa^\dagger V^\dagger = VV^\dagger = \pi(V)$).

Now the set

$$\{U(m), St_m(\mathcal{H}), \pi, Gr_m(\mathcal{H})\}, \tag{6.5}$$

is called a (universal) principal $U(m)$ bundle, see [18] and [5]. We set

$$E_m(\mathcal{H}) \equiv \{(X, v) \in Gr_m(\mathcal{H}) \times \mathcal{H} |\ Xv = v\}. \tag{6.6}$$

Then we have also a projection

$$\pi : E_m(\mathcal{H}) \to Gr_m(\mathcal{H}) \ , \quad \pi((X, v)) \equiv X. \tag{6.7}$$

The set

$$\{\mathbf{C}^m, E_m(\mathcal{H}), \pi, Gr_m(\mathcal{H})\}, \tag{6.8}$$

is called a (universal) $m$-th vector bundle. This vector bundle is associated with the principal $U(m)$ bundle (6.5).

Next let $M$ be a finite or infinite dimensional differentiable manifold and the map $P : M \to Gr_m(\mathcal{H})$ be given (called a projector). Using this $P$ we can define the pullback bundles over $M$ from (6.5) and (6.8):

$$\left\{U(m), \widetilde{St}, \pi_{\widetilde{St}}, M\right\} \equiv P^* \{U(m), St_m(\mathcal{H}), \pi, Gr_m(\mathcal{H})\}, \tag{6.9}$$

$$\left\{\mathbf{C}^m, \widetilde{E}, \pi_{\widetilde{E}}, M\right\} \equiv P^* \{\mathbf{C}^m, E_m(\mathcal{H}), \pi, Gr_m(\mathcal{H})\}, \tag{6.10}$$

see [18]. Of course the second bundle (6.10) is a vector bundle associated with the first one (6.9):

$$\begin{tikzcd}
U(m) \arrow[d] & U(m) \arrow[d] & & \mathbf{C}^m \arrow[d] & \mathbf{C}^m \arrow[d] \\
\widetilde{St} \arrow[r] \arrow[d] & St_m(\mathcal{H}) \arrow[d] & & \widetilde{E} \arrow[r] \arrow[d] & E_m(\mathcal{H}) \arrow[d] \\
M \arrow[r, "P"] & Gr_m(\mathcal{H}) & & M \arrow[r, "P"] & Gr_m(\mathcal{H})
\end{tikzcd}$$

Let $\mathcal{M}$ be a parameter space (a complex manifold in general) and we denote by $\lambda$ its element. Let $\boldsymbol{\lambda_0}$ be a fixed reference point of $\mathcal{M}$. Let $H_\lambda$ be a family of Hamiltonians parameterized by $\mathcal{M}$ acting on the Fock space $\mathcal{H}$. We set $H_0 = H_{\boldsymbol{\lambda_0}}$ for simplicity and assume that this has an $m$-fold degenerate vacuum:

$$H_0 v_j = \mathbf{0}, \quad j = 1, \ldots, m. \tag{6.11}$$

These $v_j$'s form an $m$-dimensional vector space. We may assume that $\langle v_i|v_j\rangle = \delta_{ij}$. Then $(v_1, \cdots, v_m) \in St_m(\mathcal{H})$ and

$$F_0 \equiv \left\{ \sum_{j=1}^{m} x_j v_j | x_j \in \mathbf{C} \right\} \cong \mathbf{C}^m.$$

Namely, $F_0$ is a vector space associated with the o.n. basis $(v_1, \cdots, v_m)$.

Next we assume for simplicity that a family of unitary operators parameterized by $\mathcal{M}$

$$W : \mathcal{M} \to U(\mathcal{H}), \quad W(\lambda_{\mathbf{0}}) = \text{identity}, \tag{6.12}$$

connects $H_\lambda$ and $H_0$ isospectrally:

$$H_\lambda \equiv W(\lambda) H_0 W(\lambda)^{-1}. \tag{6.13}$$

In this case there is no level crossing of eigenvalues. Making use of $W(\lambda)$ we can define a projector

$$P : \mathcal{M} \to Gr_m(\mathcal{H}), \quad P(\lambda) \equiv W(\lambda) \left( \sum_{j=1}^{m} v_j v_j^\dagger \right) W(\lambda)^{-1} \tag{6.14}$$

and the pullback bundles over $\mathcal{M}$:

$$\left\{ U(m), \widetilde{St}, \pi_{\widetilde{St}}, \mathcal{M} \right\}, \quad \left\{ \mathbf{C}^m, \widetilde{E}, \pi_{\widetilde{E}}, \mathcal{M} \right\}. \tag{6.15}$$

For the latter we set

$$|vac\rangle = (v_1, \cdots, v_m). \tag{6.16}$$

In this case a canonical connection form $\mathcal{A}$ of the principal bundle $\left\{ U(m), \widetilde{St}, \pi_{\widetilde{St}}, \mathcal{M} \right\}$ is given by

$$\mathcal{A} = \langle vac|W(\lambda)^{-1} dW(\lambda)|vac\rangle, \tag{6.17}$$

where $d$ is a differential form on $\mathcal{M}$

$$d = \sum_k \left( d\lambda_k \frac{\partial}{\partial \lambda_k} + d\bar{\lambda}_k \frac{\partial}{\partial \bar{\lambda}_k} \right)$$

together with its curvature form (see [27] and [18])

$$\mathcal{F} \equiv d\mathcal{A} + \mathcal{A} \wedge \mathcal{A}. \tag{6.18}$$

Let $\gamma$ be a loop in $\mathcal{M}$ at $\lambda_{\mathbf{0}}$, $\gamma : [0,1] \to \mathcal{M}, \gamma(0) = \gamma(1) = \lambda_{\mathbf{0}}$. For this $\gamma$ a holonomy operator $\Gamma_{\mathcal{A}}$ is defined:

$$\Gamma_{\mathcal{A}}(\gamma) = \mathcal{P}exp \left\{ \oint_\gamma \mathcal{A} \right\} \in U(m), \tag{6.19}$$

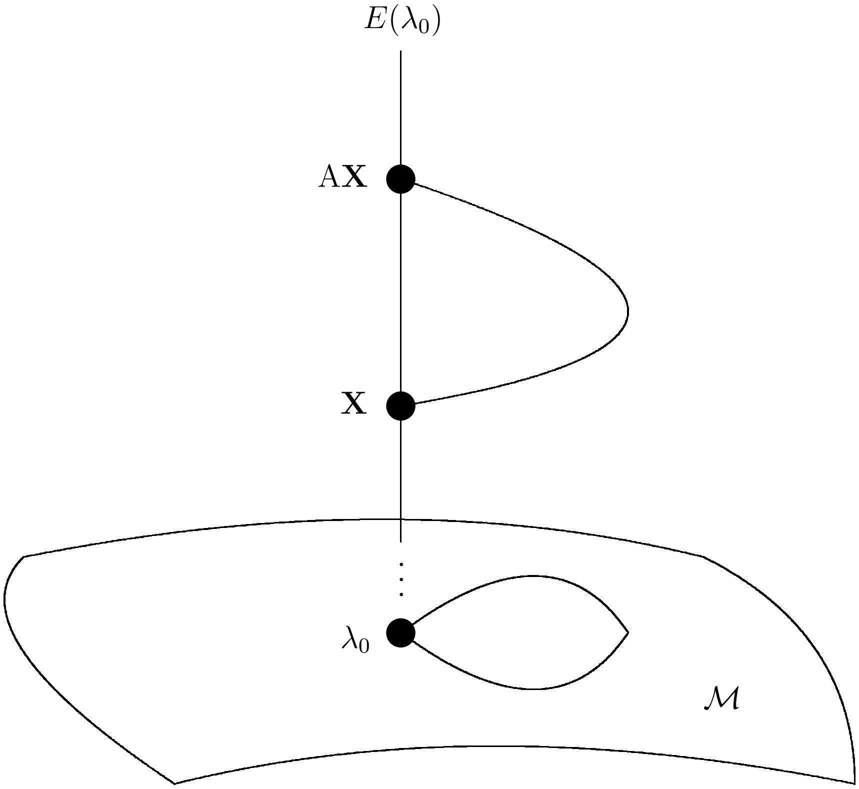
where $\mathcal{P}$ means path-ordering, see for example [21]. This acts on the fiber $F_0$ at $\lambda_{\mathbf{0}}$ of the vector bundle $\left\{ \mathbf{C}^m, \widetilde{E}, \pi_{\widetilde{E}}, M \right\}$ as follows: $\mathbf{x} \to \Gamma_{\mathcal{A}}(\gamma)\mathbf{x}$. The holonomy group $Hol(\mathcal{A})$ is in general a subgroup of $U(m)$ . In the case of $Hol(\mathcal{A}) = U(m)$, $\mathcal{A}$ is called irreducible.

The irreducibility of $\mathcal{A}$ is very important because it means the universality of quantum computation. To check whether $\mathcal{A}$ is irreducible or not we need its curvature form (6.18), see [18].

In the Holonomic Quantum Computation we take

$$\begin{aligned}&\text{Encoding of Information} \Longrightarrow \mathbf{x} \in F_0, \\ &\text{Processing of Information} \Longrightarrow \Gamma_{\mathcal{A}}(\gamma) : \mathbf{x} \rightarrow \Gamma_{\mathcal{A}}(\gamma)\mathbf{x} \equiv A\mathbf{x}.\end{aligned} \tag{6.20}$$

See the following figure.



Our model is relatively complicated compared to the other geometric models and much more so than the usual spin models. We have a lot of problems to solve in the near future. We strongly hope young graduate students to invigorate this field.

*Acknowledgment.* The author wishes to thank Yoshinori Machida for his warm hospitality at Numazu College of Technology. I also wishes to thank Akira Asada, Ryu Sasaki and Tatsuo Suzuki for reading this manuscript and making some useful comments.

# Appendix

## A. A Family of Flag Manifolds

Let us make a comment on an interesting relation between flag manifolds and the kernel of the exponential map defined on matrices. Here a (generalized) flag manifold (which is

a useful manifold as shown in the following) is a natural generalization of the Grassmann one.
First of all we make a brief review. For

$$\exp : \mathbf{R} \longrightarrow S^1 \ \subset \ \mathbf{C}, \quad \exp(t) \equiv \mathrm{e}^{2\pi\sqrt{-1}t}$$

the kernel of this map is ker(exp)=$\mathbf{Z} \ \subset \ \mathbf{R}$.

We define by $H(n, \mathbf{C})$ the set of all hermitian matrices

$$H(n, \mathbf{C}) = \{X \in M(n, \mathbf{C}) \mid X^\dagger = X\}.$$

Of course $H(1, \mathbf{C}) = \mathbf{R}$. Note that each element of $H(n, \mathbf{C})$ can be diagonalized by some unitary matrix.
The exponential map is now defined as

$$\mathrm{E} : H(n, \mathbf{C}) \longrightarrow U(n), \quad \mathrm{E}(X) = \mathrm{e}^{2\pi\sqrt{-1}X}. \tag{A.1}$$

Here our target is ker(E).

**Problem** What is the structure of ker(E) ?

Our claim is that ker(E) is a family of flag manifolds. For that we write ker(E) as

$$K_n(\mathbf{C}) = \{X \in H(n, \mathbf{C}) \mid \mathrm{e}^{2\pi\sqrt{-1}X} = \mathbf{1}_n\}. \tag{A.2}$$

First we prove

$$G_n(\mathbf{C}) \ \subset \ K_n(\mathbf{C}). \tag{A.3}$$

Because since $P^2 = P$ from the definition, $P^k = P$ for $k \geq 1$, so that

$$\mathrm{e}^{2\pi\sqrt{-1}P} = \mathbf{1}_n + \sum_{k=1}^{\infty} \frac{(2\pi\sqrt{-1})^k}{k!} P^k = \mathbf{1}_n + \sum_{k=1}^{\infty} \frac{(2\pi\sqrt{-1})^k}{k!} P = \mathbf{1}_n + (\mathrm{e}^{2\pi\sqrt{-1}} - 1)P = \mathbf{1}_n. \tag{A.4}$$

We will prove that $G_n(\mathbf{C})$ becomes a kind of basis for $K_n(\mathbf{C})$.
For $X \in K_n(\mathbf{C})$ we write the set of all eigenvalues of $X$ as spec$(X)$. Then spec$(X) = \{0, 1\}$ for $X \in G_n(\mathbf{C})$.
It is clear that spec$(X) \subset \mathbf{Z}$. For $X \in K_n(\mathbf{C})$ we have

$$\mathrm{spec}(X) = \{n_1(d_1), \ \cdots, \ n_k(d_k), \ \cdots, n_j(d_j)\} \quad \text{where} \quad n_k \in \mathbf{Z} \text{ and } \sum_{k=1}^{j} d_k = n, \tag{A.5}$$

in which $(d_k)$ is the multiplicity of the eigenvalue $n_k$. Since $X$ is diagonalized by some $U \in U(n)$,

$$X = UX_0U^{-1} = \sum_{k=1}^{j} n_k P_{d_k}, \tag{A.6}$$

where

$$X_0 = \begin{pmatrix} n_1\mathbf{1}_{d_1} & & & & \\ & n_2\mathbf{1}_{d_2} & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & n_j\mathbf{1}_{d_j} \end{pmatrix}, \quad P_{d_k} = U \begin{pmatrix} \mathbf{0}_{d_1} & & & & \\ & \cdot & & & \\ & & \mathbf{1}_{d_k} & & \\ & & & \cdot & \\ & & & & \mathbf{0}_{d_j} \end{pmatrix} U^{-1}. \tag{A.7}$$

Here we list some properties of the set of projections $\{P_{d_k}\}$:

$$(1) \quad P_{d_k} \in G_{d_k,n}(\mathbf{C}), \quad (2) \quad P_{d_k}P_{d_l} = \delta_{kl}P_{d_l}, \quad (3) \quad P_{d_1} + P_{d_2} + \cdots + P_{d_j} = \mathbf{1}_n.$$

Let us here prepare a terminology. For $X \in K_n(\mathbf{C})$ we call set of the eigenvalues together with multiplicities

$$\{(n_1, d_1), (n_2, d_2), \cdots, (n_j, d_j)\}$$

the spectral type of $X$.
Then it is easy to see that $X$ and $Y \in K_n(\mathbf{C})$ are of the same spectral type ($X \sim Y$) if and only if $Y = UXU^{-1}$ for some $U \in U(n)$. For $X \in K_n(\mathbf{C})$ we define

$$C(X) = \{Y \in K_n(\mathbf{C}) \mid Y \sim X\} \ .$$

We have clearly $C(X) = C(X_0)$. Then it is easy to see that $K_n(\mathbf{C})$ can be classified by the spectral type

$$K_n(\mathbf{C}) = \bigcup_X C(X) = \bigcup_{X_0} C(X_0) \tag{A.8}$$

and the unitary group $U(n)$ acts on $C(X)$ as follows:

$$U(n) \times C(X) \longrightarrow C(X) \ : \ (U, X) \mapsto UXU^{-1}.$$

Since this action is free and transitive, the isotropy group at $X_0$ is

$$U(d_1) \times U(d_2) \times \cdots \times U(d_j) \ ,$$

so that we have

$$C(X) \cong \frac{U(n)}{U(d_1) \times U(d_2) \times \cdots \times U(d_j)} \ . \tag{A.9}$$

The right hand side is called a generalized flag manifold. In particular when $d_1 = d_2 = \cdots = d_n = 1$ (there is no overlapping in the eigenvalues of X) we have

$$C(X) \cong \frac{U(n)}{U(1) \times U(1) \times \cdots \times U(1)} \ . \tag{A.10}$$

This is called a flag manifold.
Namely by (A.8) we know that $K_n(\mathbf{C})$ is a family of generalized flag manifolds.

A comment is in order. For the Grassmann manifolds we have very good local coordinates like (2.8), while we don't know good local coordinates for generalized flag manifolds.

**Problem** Find a good local coordinate system.

For some applications of generalized flag manifolds the paper [23] is recommended. See also [23] and references therein.

# B. A Generalization of Pauli Matrices

Here let us introduce a generalization of Pauli matrices (5.15) which has been used in several situations in both Quantum Field Theory and Quantum Computation.

First of all we summarize the properties of Pauli matrices. By (5.15) $\sigma_2 = \sqrt{-1}\sigma_1\sigma_3$, so that the essential elements of Pauli matrices are $\{\sigma_1, \sigma_3\}$ and they satisfy

$$\sigma_1^2 = \sigma_3^2 = \mathbf{1}_2; \qquad \sigma_1^\dagger = \sigma_1,\ \sigma_3^\dagger = \sigma_3; \qquad \sigma_3\sigma_1 = -\sigma_1\sigma_3. \tag{B.1}$$

Let $\{\Sigma_1, \Sigma_3\}$ be the following matrices in $M(n, \mathbf{C})$

$$\Sigma_1 = \begin{pmatrix} 0 & & & & & 1 \\ 1 & 0 & & & & \\ & 1 & 0 & & & \\ & & 1 & \cdot & & \\ & & & \cdot & \cdot & \\ & & & & \cdot & \cdot \\ & & & & 1 & 0 \end{pmatrix}, \qquad \Sigma_3 = \begin{pmatrix} 1 & & & & & & \\ & \sigma & & & & & \\ & & \sigma^2 & & & & \\ & & & \cdot & & & \\ & & & & \cdot & & \\ & & & & & \cdot & \\ & & & & & & \sigma^{n-1} \end{pmatrix} \tag{B.2}$$

where $\sigma$ is a primitive root of unity $\sigma^n = 1$ ( $\sigma = \mathrm{e}^{\frac{2\pi\sqrt{-1}}{n}}$). We note that

$$\bar{\sigma} = \sigma^{n-1}, \quad 1 + \sigma + \cdots + \sigma^{n-1} = 0.$$

The two matrices $\{\Sigma_1, \Sigma_3\}$ are generalizations of Pauli matrices $\{\sigma_1, \sigma_3\}$, but they are not hermitian. Here we list some of their important properties:

$$\Sigma_1^n = \Sigma_3^n = \mathbf{1}_n \quad ; \quad \Sigma_1^\dagger = \Sigma_1^{n-1},\ \Sigma_3^\dagger = \Sigma_3^{n-1} \quad ; \quad \Sigma_3\Sigma_1 = \sigma\Sigma_1\Sigma_3\ . \tag{B.3}$$

If we define a Vandermonde matrix $W$ based on $\sigma$ as

$$W = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & \cdot\ \cdot\ \cdot & 1 \\ 1 & \sigma^{n-1} & \sigma^{2(n-1)} & \cdot\ \cdot\ \cdot & \sigma^{(n-1)^2} \\ 1 & \sigma^{n-2} & \sigma^{2(n-2)} & \cdot\ \cdot\ \cdot & \sigma^{(n-1)(n-2)} \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ 1 & \sigma^2 & \sigma^4 & \cdot\ \cdot\ \cdot & \sigma^{2(n-1)} \\ 1 & \sigma & \sigma^2 & \cdot\ \cdot\ \cdot & \sigma^{n-1} \end{pmatrix}, \tag{B.4}$$

$$W^\dagger = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & \cdot\ \cdot\ \cdot & 1 \\ 1 & \sigma & \sigma^2 & \cdot\ \cdot\ \cdot & \sigma^{n-1} \\ 1 & \sigma^2 & \sigma^4 & \cdot\ \cdot\ \cdot & \sigma^{2(n-1)} \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ 1 & \sigma^{n-2} & \sigma^{2(n-2)} & \cdot\ \cdot\ \cdot & \sigma^{(n-1)(n-2)} \\ 1 & \sigma^{n-1} & \sigma^{2(n-1)} & \cdot\ \cdot\ \cdot & \sigma^{(n-1)^2} \end{pmatrix}, \tag{B.5}$$

then it is not difficult to see

$$\Sigma_1 = W\Sigma_3W^\dagger = W\Sigma_3W^{-1}. \tag{B.6}$$

For example, for $n = 3$

$$
\begin{aligned}
W\Sigma_3 W^\dagger &= \frac{1}{3}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \sigma^2 & \sigma \\ 1 & \sigma & \sigma^2 \end{pmatrix}\begin{pmatrix} 1 & & \\ & \sigma & \\ & & \sigma^2 \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \sigma & \sigma^2 \\ 1 & \sigma^2 & \sigma \end{pmatrix} \\
&= \frac{1}{3}\begin{pmatrix} 1 & \sigma & \sigma^2 \\ 1 & 1 & 1 \\ 1 & \sigma^2 & \sigma \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \sigma & \sigma^2 \\ 1 & \sigma^2 & \sigma \end{pmatrix} = \frac{1}{3}\begin{pmatrix} 0 & 0 & 3 \\ 3 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix} = \Sigma_1,
\end{aligned}
$$

where we have used that $\sigma^3 = 1,\ \bar{\sigma} = \sigma^2$ and $1 + \sigma + \sigma^2 = 0$.
That is, $\Sigma_1$ can be diagonalized by making use of $W$.
A comment is in order. Since $W$ corresponds to the Walsh-Hadamard matrix (5.12), so it may be possible to call $W$ the generalized Walsh-Hadamard matrix.

# C. General Controlled Unitary Operations

Here let us introduce a usual construction of general controlled unitary operations to help the understanding of general controlled NOT one. In the following arguments if we take $U = X = \sigma_1$ then they reduce to the arguments of a construction of general controlled NOT operator.

First of all let us recall (5.27). For $x, y, z \in \mathbf{Z}_2$ we have identities :

$$x + y - x \oplus y = 2xy, \tag{C.1}$$

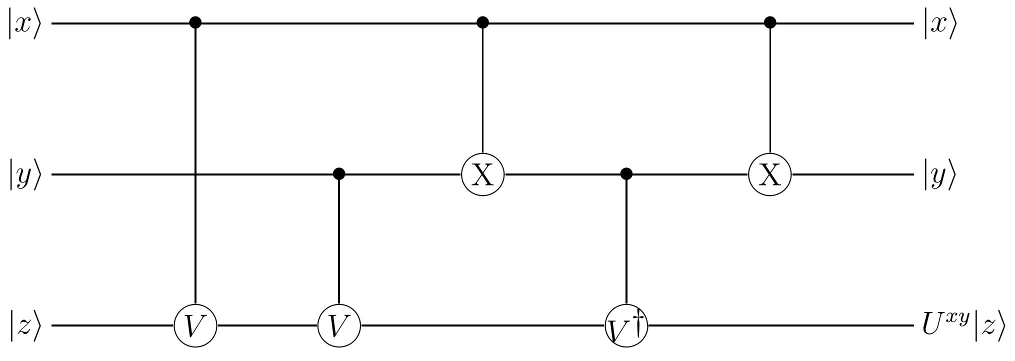
$$x + y + z - x \oplus y - x \oplus z - y \oplus z + x \oplus y \oplus z = 4xyz, \tag{C.2}$$

where $x \oplus y = x + y \pmod 2$. For the most general identities of above type see [1] and [9].
The controlled-controlled unitary operations are constructed by making use of both several controlled unitary operations and controlled NOT operations: Let $U$ be an arbitrarily unitary matrix in $U(2)$ and $V$ a unitary one in $U(2)$ satisfying $V^2 = U$. Then by (C.1) we have

$$V^{x+y-x\oplus y} = V^{2xy} = (V^2)^{xy} = U^{xy}, \tag{C.3}$$

$$V^{x+y-x\oplus y} = V^x V^y V^{-x\oplus y} = V^x V^y (V^{-1})^{x\oplus y} = V^x V^y (V^\dagger)^{x\oplus y}, \tag{C.4}$$

so a controlled-controlled $U$ operation is graphically represented as



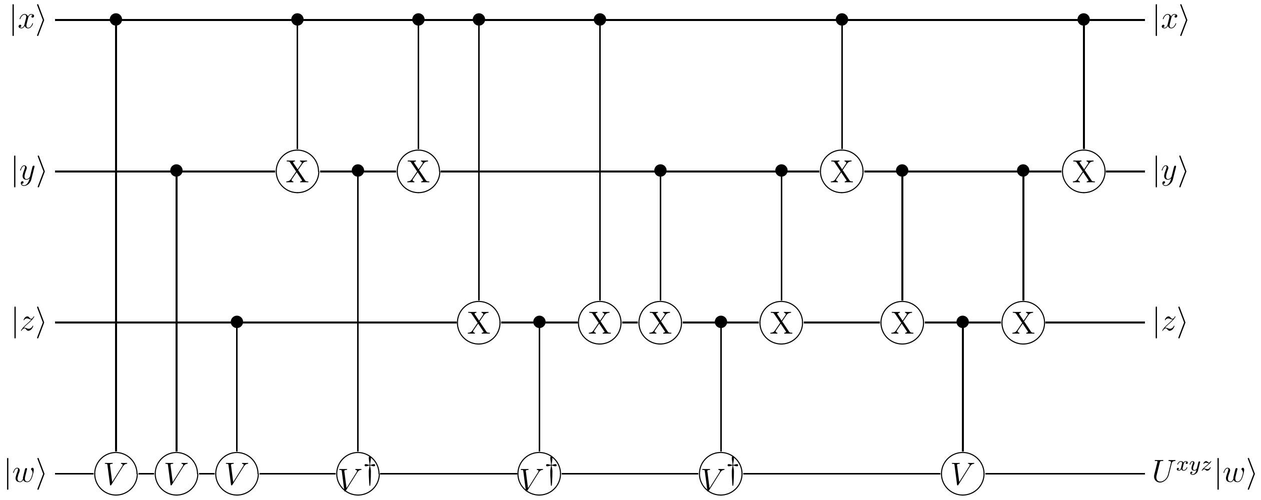
You should read this figure as follows: From the left to the right

$$|x\rangle \otimes |y\rangle \otimes |z\rangle \;\longrightarrow\; |x\rangle \otimes |y\rangle \otimes U^{xy}|z\rangle.$$

The controlled-controlled-controlled unitary operations are constructed as follows: Let $U$ be an arbitrarily unitary matrix in $U(2)$ and $V$ be a unitary one in $U(2)$ satisfying $V^4 = U$. Then by (C.1)

$$\begin{aligned} V^{x+y+z-(x\oplus y+x\oplus z+y\oplus z)+x\oplus y\oplus z} &= V^{4xyx} = U^{xyz}, && \text{(C.5)} \\ V^{x+y+z-(x\oplus y+x\oplus z+y\oplus z)+x\oplus y\oplus z} &= V^xV^yV^z(V^\dagger)^{x\oplus y}(V^\dagger)^{x\oplus z}(V^\dagger)^{y\oplus z}V^{x\oplus y\oplus z}, && \text{(C.6)} \end{aligned}$$

so a controlled-controlled-controlled $U$ operation is graphically represented as



This figure means

$$|x\rangle \otimes |y\rangle \otimes |z\rangle \otimes |w\rangle \;\longrightarrow\; |x\rangle \otimes |y\rangle \otimes |z\rangle \otimes U^{xyz}|w\rangle.$$

A comment is in order. For the case $U = X = \sigma_1$ we have from (5.39)

$$\begin{aligned} |a_1, a_2, \cdots, a_{n-1}, a_n\rangle \;\longrightarrow & |a_1, a_2, \cdots, a_{n-1}, a_1a_2\cdots a_{n-1} \oplus a_n\rangle \\ \equiv & |a_1\rangle \otimes |a_2\rangle \otimes \cdots |a_{n-1}\rangle \otimes |a_1a_2\cdots a_{n-1} \oplus a_n\rangle \\ = & |a_1\rangle \otimes |a_2\rangle \otimes \cdots |a_{n-1}\rangle \otimes X^{a_1a_2\cdots a_{n-1}}|a_n\rangle. \qquad \text{(C.7)} \end{aligned}$$

As can be seen from the figures the well-known construction of general controlled unitary operations needs exponential steps. Namely it is not efficient. For more details see [1] and [9].

# References

[1] A. Barenco, C. H. Bennett, R. Cleve, D. P. Vincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin and H. Weinfurter : Elementary gates for quantum computation, Phys. Rev. **A 52** (1995), 3457, quant-ph/9503016.

[2] G. Chen and Z. Diao : Exponentially fast quantum search algorithm, quant-ph/0011109.

[3] D. Deutsch, A. Barenco and A. Eckert : Universality in Quantum Computation, Proc. Roy. Soc. London **A 474** (1995), 969, quant-ph/9505018.

[4] G. Dunne : Self-Dual Chern–Simons Theories, Lecture Notes in Physics, m 36, 1995, Springer.

[5] K. Fujii : Note on Coherent States and Adiabatic Connections, Curvatures, J. Math. Phys. **41** (2000), 4406, quant-ph/9910069.

[6] K. Fujii : Mathematical Foundations of Holonomic Quantum Computer, Rept. Math. Phys. **48** (2001), 75, quant-ph/0004102.

[7] K. Fujii : More on Optical Holonomic Quantum Computer, quant-ph/0005129.

[8] K. Fujii : Mathematical Foundations of Holonomic Quantum Computer II, quant-ph/0101102.

[9] K. Fujii : A Lecture on Quantum Logic Gates, The Bulletin of Yokohama City University, **53** (2002), 1, quant-ph/0101054.

[10] K. Fujii, T. Kashiwa, S. Sakoda :Coherent states over Grassmann manifolds and the WKB exactness in path integral, J. Math. Phys. **37** (1996), 567.

[11] K. Funahashi : a private communication.

[12] L. K. Grover : A framework for fast quantum mechanical algorithms, Proceedings of the 30th annual ACM symposium on the theory of computing, 1998, 53, quant-ph/9711043.

[13] A. Hosoya : Lectures on Quantum Computation (in Japanese), 1999, Science Company (in Japanese).

[14] R. Jozsa : Quantum Algorithms and the Fourier Transform, in Proceedings of Santa Barbara Conference on Quantum Coherence and Decoherence, quant-ph/9707033.

[15] R. Jozsa : Quantum factoring, discrete logarithms and the hidden subgroup problem, in special issue of ”IEEE Computing in Science and Engineering”, quant-ph/0012084.

[16] A. Yu. Kitaev : Fault–tolerant quantum computation by anyons, quant-ph/9707021.

[17] H. K. Lo, S. Popescu and T. Spiller (Eds) : Introduction to quantum computation and information, World Scientific, Singapore, 1999.

[18] M. Nakahara : Geometry, Topology and Physics, IOP Publishing Ltd, 1990.

[19] H. Oike : Geometry of Grassmann Manifolds (in Japanese), Lecture Note, Yamagata University, 1979.

[20] J. Pachos and S. Chountasis : Optical Holonomic Quantum Computer, Phys. Rev. **A 62** (2000), 052318, quant-ph/9912093.

[21] J. Pachos and P. Zanardi : Quantum Holonomies for Quantum Computing, quant-ph/0007110.

[22] J. Pachos, P. Zanardi and M. Rasetti : Non–Abelian Berry connections for quantum computation, Phys. Rev. **A 61** (2000), 010305(R), quant-ph/9907103.

[23] R. F. Picken : The Duistermaat–Heckman integration formula on flag manifolds, J. Math. Phys. **31** (1990), 616.

[24] J. Preskill : Fault–Tolerant Quantum Computation, in [17], quant-ph/9712048.

[25] S. G. Rajeev, S. K. Rama and S. Sen : Symplectic Manifolds, Coherent States and Semiclassical Approximation, J. Math. Phys. **35** (1994), 2259, hep-th/9310138.

[26] E. Rieffel and W. Polak : An Introduction to Quantum Computing for Non-Physicists, To appear in ACM Computing Surveys, quant-ph/9809016.

[27] A. Shapere and F. Wilczek (Eds) : Geometric Phases in Physics, World Scientific, Singapore, 1989.

[28] P. W. Shor : Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Computing., **26** (1997), 1484, quant-ph/9508027.

[29] A. Steane : Quantum Computing, Rept. Prog. Phys., **61** (1998), 117, quant-ph/9708022 .

[30] W. J. Zakrzewski : Low Dimensional Sigma Models, 1989, Adam-Hilger.

[31] P. Zanardi and M. Rasetti : Holonomic Quantum Computation, Phys. Lett. **A 264** (1999), 94, quant-ph/9904011.